ABSTRACT

SP6
Cyber Risk & Compliance

Continuous Controls Monitoring in CMMC Level 2 Compliance:

An In-Depth Exploration of Control 3.12.3

In CMMC, continuous monitoring stands as a pivotal component in safeguarding sensitive information. For organizations aiming to achieve Cybersecurity Maturity Model Certification (CMMC) Level 2 compliance, a thorough understanding and implementation of 'continuous monitoring' and its role in Risk Management is essential.

It is easy to conflate three closely related topics, Continuous Controls Monitoring (CCM), Information Security Continuous Monitoring (ISCM), and Risk Monitoring and Management (Risk Management Framework or RMF).

This white paper delves into these topics, emphasizing their significance in the context of CMMC Level 2, with a particular focus on Control 3.12.3 as outlined in NIST SP 800-171. Furthermore, it integrates insights from NIST SP 800-137 to provide a comprehensive perspective on establishing and maintaining an effective continuous monitoring program.

1. Introduction

The Department of Defense (DoD) introduced the CMMC framework to enhance the protection of Controlled Unclassified Information (CUI) within the Defense Industrial Base (DIB). Achieving Level 2 compliance necessitates adherence to the 110 security requirements specified in NIST SP 800-171. Among these requirements (also known as controls), control 3.12.3 mandates organizations to *"monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls."* This control underscores the importance of continuous monitoring in maintaining a robust security posture.

2. Understanding Continuous Monitoring

In the abstract, we mentioned three related terms. Let's start by defining and differentiating between them:

- Continuous Controls Monitoring
- Continuous Monitoring (Information Security Continuous Monitoring)
- Risk Monitoring in the context of the NIST Risk Management Framework

Continuous Controls Monitoring - A means to determine if a control is implemented as designed and functioning as designed, on an ongoing basis.

Example for the need: A control is compliant if it is meeting the requirements as defined in the security standard (in the case of CMMC, NIST 800-171). A control can start as compliant and become non-compliant over time. This could be from a change in the configuration of a product or service used to meet a requirement, or failure to consistently perform operational procedures such as change control, not updating baselines after a change is made, failure to consistently run vulnerability scans, etc. The point being, most requirements are not set and forget. We monitor controls to ensure that they have not inadvertently gone out of compliance over time.

While some sources may use CCM and continuous monitoring interchangeably, CCM specifically refers to using technology-based solutions to automate and constantly evaluate whether security controls are present and functioning correctly. This often involves monitoring the performance of the controls themselves, such as verifying antivirus updates or tracking security configurations.

ISCM in contrast, is monitoring for control effectiveness. Control effectiveness takes us into the area of risk management. ISCM involves maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM focuses on the overall process and strategy of ongoing monitoring of security controls and organizational risk.

In essence, CCM is a way to *implement* ISCM in a more efficient and effective manner, especially for monitoring technical controls. By leveraging automated tools for CCM, organizations can get near real-time insights into their security posture, enabling them to make more informed risk management decisions and better respond to emerging threats as part of their larger ISCM strategy.

Some readers may have noted the apparent contradiction – why monitor control effectiveness continuously (control 3.12.3), but only assess risk periodically (control 3.11.1)? The reason that both are required is that Risk is dynamic. While the controls may be effective at mitigating risk based on Risk as previously defined, underlying Risk elements (threats, vulnerabilities to those threats, and the impact of those threats being realized) will change over time.

In compliance with 800-171, we periodically reassess Risk. At the completion of this reassessment, we may need to change a control's design to ensure effectiveness. In between these more comprehensive Risk reviews, we employ ISCM to monitor the effectiveness of the controls we've chosen to reduce the risks identified in our previous risk assessment.

According to NIST SP 800-137, an Information Security Continuous Monitoring (ISCM) program provides ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The primary objectives of continuous monitoring include:

- **Ongoing Assessment:** Regular evaluation of security controls to verify their proper implementation and effectiveness.

- **Threat Awareness:** Maintaining up-to-date knowledge of potential threats and vulnerabilities that could impact the organization.
- **Risk Management Support:** Providing actionable insights to inform risk-based decision-making processes.

Put that all together and you get—an effective ISCM can provide an early warning system that a control (or controls) are not effectively keeping risk at an acceptable level, *in between periodic Risk Assessments*.

3. Control 3.12.3 in NIST SP 800-171

Control 3.12.3 specifically requires organizations to monitor security controls continuously to ensure their ongoing effectiveness (or as discussed above, in between Risk Assessments). The terms "continuous" and "ongoing" imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Automation supports more frequent updates to hardware, software, firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Monitoring requirements, including the need for specific monitoring, may also be referenced in other requirements. NIST SP 800-137 provides guidance on continuous monitoring.

4. Implementing Continuous Monitoring for CMMC Level 2 Compliance

To align with Control 3.12.3 and achieve CMMC Level 2 compliance, organizations should consider the following steps:

- **Develop an ISCM Strategy:** Establish a formal strategy that defines the scope, objectives, and methodologies for continuous monitoring, tailored to the organization's risk tolerance and operational environment.
- **Establish an ISCM Program:** Implement a structured program that includes policies, procedures, and technologies to support continuous monitoring activities.
- **Define Metrics and Frequencies:** Identify specific metrics to assess the effectiveness of security controls and determine the frequency of monitoring activities based on the criticality of assets and potential impact of threats.
- **Leverage Automation:** Utilize CCM automated tools (such as ASCERA) to facilitate real-time data collection, analysis, and reporting, enhancing the efficiency and accuracy of monitoring efforts.
- **Analyze and Respond:** Regularly analyze collected data to identify anomalies or deviations from expected behavior and implement appropriate responses to mitigate identified risks.
- **Review and Update:** Continuously **review and refine** the ISCM strategy and program to adapt to evolving threats, technologies, and organizational changes.

5. Challenges and Considerations

Implementing an effective continuous monitoring program presents several challenges:

- **Resource Allocation:** Ensuring adequate resources, including personnel and technology, to support continuous monitoring efforts.
- **Data Overload:** Managing and analyzing large volumes of data generated by monitoring tools to extract meaningful insights.
- **Integration:** Ensuring seamless integration of continuous monitoring tools with existing security infrastructure and processes.
- **Compliance Maintenance:** Staying in-tune regulatory changes and ensuring that continuous monitoring practices remain aligned with compliance requirements.

6. Conclusion

Continuous Controls Monitoring is a means of implementing Information Security Continuous Monitoring, a cornerstone of effective cybersecurity risk management and is integral to achieving and maintaining CMMC Level 2 compliance. By utilizing a CCM tool such as ASCERA, organizations can adhere to the guidelines set forth in NIST SP 800-137 and implementing the practices required by Control 3.12.3 of NIST SP 800-171, organizations can establish a robust continuous monitoring program effectively and without undue burden on IT and security resources. Such a program not only fulfills compliance obligations but also enhances the organization's ability to detect, respond to, and mitigate emerging threats, thereby safeguarding CUI and supporting the overall mission of the organization.

References

- National Institute of Standards and Technology. (2011). *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (SP 800-137).* **Link**
- National Institute of Standards and Technology. (2020). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (SP 800-171 Rev. 2).* **Link**
- Cybersecurity Maturity Model Certification (CMMC) Model Overview. (2021). **Link**